VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

2017 Jiří Káša

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Jiří Káša**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R059 Mobilní technologie

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: XEVOS Solutions s.r.o.
2. Struktura závěrečné zprávy:
a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta
b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti
c. Zvolený postup řešení zadaných úkolů
d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe
e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe
f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vedl odbornou praxi studenta

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**

Konzultant bakalářské práce: Adam Koudela

Datum zadání: 01.09.2016

Datum odevzdání: 28.04.2017

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * 1D16 * OSTRAVA *

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *19. dubna 2017*

.....
podpis studenta

Poděkování

Rád bych poděkoval *"Adamu Koudelovi a Ing. Zdeňce Chmelíkové Ph.D."* za odbornou pomoc a konzultaci při vytváření této bakalářské práce.

Prohlášení zástupce spolupracující právnické nebo fyzické osoby

„Souhlasím se zveřejněním této bakalářské/diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských/magisterských programech VŠB-TU Ostrava."

Dne: 11. dubna 2017

podpis zástupce

Abstrakt

Jako první úkol jsem měl vytvořit nový virtuální počítač, na který se nainstaluje operační systém Windows server 2016 a bude sloužit jakožto RADIUS server pro bezdrátovou síť firmy. Před implementací RADIUS serveru fungovala bezdrátová síť firmy pouze pomocí přístupových bodů a díky tomuto má nyní větší bezpečnost a připojí se do ní pouze uživatelé z Active Directory. Dalším úkolem bylo implementovat helpdesk, který se nyní využívá pro zpracování klientských požadavků. Dále následovaly úkoly přímo vykonané pro klienty, kde bylo potřeba využít virtuální privátní sítě a vzdáleného přístupu. Pracoval jsem se skupinovými politiky, kde bylo potřeba určit pravidla, jaké přístupy budou mít dané skupiny uživatelů. Posledním byla práce s NAS serverem, který slouží pro sdílení složek v doméně pomocí SMB protokolu.

Klíčová slova

Windows Server, Hyper-V, Helpdesk, Virtuální privátní sít, Vzdálený přístup, SMB, NAS, Skupinové politiky, Active Directory,

Abstract

As first task i had to create new virtual machine, which will contain operation systém Windows server 2016 and will work as RADIUS server for wireless network in firm. Before implementation RADIUS server, wireless network in firm was managed by access points and thanks to RADIUS it has better security and only users from Active directory can connect. Next task was to implement Helpdesk, which is now used for processing klient tickets. And next tasks was primary for clients, where I needed to connect into intern network by Virtual private network and remote desktop. I worked with Group policies, where I setup rules, which access will have specific group of users. Last work was with NAS server, which serves for shares in domain through SMB protocol.

Key words

Windows Server, Hyper-V, Helpdesk, Virtual private network, Remote desktop, SMB, NAS, Group policies, Active Directory,

Obsah

Seznam použitých zkratek

Zkratka	Význam
AD	Active Directory
AFP	Apple Filling Protocol
AP	Access Point
API	Application Programming Interface
CA	Certification Authority
CAL	Client access license
CIFS	Common Internet File System
DISM	Deployment Image Servicing and Management
GUI	Graphical User Interface
FTP	File Transfer Protocol
HCAP	Host Credential Authorization Protocol
HW	Hardware
IPC	Inter-Process Communication
ISO	International Organization for Standardization
IT	Informační technologie
NAS	Network Attached Storage
NAP	Network Access Protection
NetBIOS	Network Basic Input Output System
NFS	Network File System
OSE	Operating System Environment
OSI	Open Systems Interconnection
P2P	Peer-to-peer
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Access Dial-Up System
RDP	Remote Desktop protocol
RTF	Rich Text Format
SID	Security Identifier
SLA	Service-level agreement
SMB	Server Message Block
SSH	Secure Shell
SW	Software
VM	Virtual Machine
VPN	Virtual Private Network
WS	Windows Server

Seznam ilustrací a seznam tabulek

Úvod

Vykonával jsem odbornou praxi u společnosti XEVOS Solutions s.r.o, která se zabývá poskytováním profesionálních servisních služeb a systémovou integrací. Byla založena v roce 2008 a v současné době působí ve dvou lokalitách, a to v Ostravě, kde se nachází sídlo společnosti, a v Praze. Mezi primární aktivity společnosti patří především IT podpora a servis hardwarových i softwarových řešení, kde se profilují jako nezávislý servisní partner a své služby poskytují jak na pobočkách, tak především on-site přímo u zákazníků. V oblasti servisu veškerých PC zařízení, periferií a komponent vytvořili servisní centrum, ve kterém zajišťují opravy všech běžně dostupných značek na trhu. Provádí záruční i pozáruční opravy. Služby servisního centra jsou určeny nejen stálým zákazníkům, ale využívají je i drobní domácí uživatelé. Jako systémový integrátor nabízejí serverová, cloudová i klientská řešení pro firmy i domácnosti při využití platforem PC i MacOS, tiskových řešení, prezentační techniky, tabletů i chytrých telefonů.

Na začátku jsem se musel seznámit s využívaným prostředím a technologiemi jako je Hyper-v, VPN, RDP a různé typy zařízení, které jsou zmíněny v první kapitole. Druhá kapitola již obsahuje vykonávanou odbornou práci počínaje vytvořením nového virtuálního počítače, následnou implementací do interní sítě firmy jakožto doménového řadiče a nastavením služby RADIUS server. V další kapitole pojednávám o implementaci firemního helpdesku za pomocí služby IIS s podporou PHP a práce s ním. A nakonec jsem vykonával odborné úkony pro klienty, které si žádaly plnou znalost používaných služeb a funkcí, jelikož se jednalo o práci přímo na provozních serverech, kde by mohlo dojít k problémům, což by mohlo mít nežádoucí důsledky jak pro firmu, tak pro klienta. Ve čtvrté kapitole jsem řešil problematiku skupinových politik. Bylo potřeba vytvořit pravidla pro uživatelská oprávnění. V páté kapitole popisuji práci na na NAS serveru, kde jsem vytvářel sdílené složky pro doménu a nastavoval přístup pro uživatele z domény.

1 Využité Technologie

1.1 Windows Server

Windows Server je operační systém z řady Windows NT. V dnešní době se již používá nejnovější verze WS 2016, která navazuje na WS 2012 R2. Stále se používají i starší verze, ale ty už nejsou podporovány novými aktualizacemi, kromě WS 2012/2012R2. Porovnání rozdílů mezi WS 2012/2012R2 a WS 2016 je znázorněno v tabulce. [1]

Tabulka 1.1: *Porovnání WS 2012/R2 a WS 2016*

Výkon a škálovatelnost	WS 2012/R2 Datacenter a Standard	WS 2016 Datacenter a Standard
Podpora fyzické (hostované) paměti	Až 4TB na fyzický server	Až 24TB na fyzický server
Podpora fyzického (hostovaného) logického procesoru	Až 320	Až 512
Podpora paměti VP	Až 1TB na VP	Až 12TB na VP
Podpora virtuálních procesorů VP	Až 64 na VP	Až 240 na VP

Dále se již bude jednat pouze o verzi WS 2016. Existují 3 edice licencí Datacenter, Standard a Essentials. Rozdíl mezi nimi je v celku podstatný jak ve funkcionalitě, tak v ceně. Datacenter se používá pro vysoce virtualizovaná prostředí, a to privátních i hybridních cloudů. Standard je určen pro ne-virtualizovaná prostředí, ale lze jej použít i na lehce virtualizované prostředí. Liší se tím, že má omezený počet Hyper-v konterjnérů oproti Datacenter licenci a také je výrazně levnější. Licence Essentials je určena pro malé podniky s maximálním počtem uživatelů 25 a s 50 zařízeními. Porovnání edic je v následující tabulce. [2] [3]

Tabulka 1.2: *Rozdíly edic v systému Windows server 2016*

Edice Windows Serveru 2016	Datacenter	Standard
Základní funcionality WS	x	x
OSEs/Hyper-V kontejnery	Neomezeno	2
WS kontejnery	Neomezeno	Neomezeno
Nano Server	x	x
Nové Možnosti ukládání dat a to včetně Storage Spaces Direct a Storage Replica	x	
Nové verze Shielded Virtual Machines a Host Guardian Service	x	
Nový síťový stack	x	

Pro Datacenter a Standard je licenční politika závislá na počtu fyzických jader serveru a CAL. Na každý fyzický procesor je požadováno minimálně 8 licencí na jádro a na každý fyzický server je potřeba minimálně 16 licencí na jádro. U licence Essentials je model licencování na základě procesoru bez potřeby CAL.

1.1.1 Nano server

Jedná se o minimalistickou verzi WS bez GUI. Primárně je určen jako systém hostující cloudové aplikace. Díky tomu byl zredukován o nepotřebné služby a funkce systému a je optimalizován pro datová centra. Pro počáteční konfiguraci se využívá DISM a na vzdálenou konfiguraci běžícího systému je využit Telnet nebo PowerShell. Díky podpoře Group Policy je možné připojit Nano server do domény jakožto člena. [4]

1.2 Hyper-V

Tato technologie je vytvořena společností Microsoft sloužící pro virtualizaci. Hlavní komponentou této technologie je Hypervisor umožňující rozdělení HW na logické jednotky a tím tvoří virtuální vrstvu. Umožňuje podporu více současně běžících OS na jednom serveru. Jednotlivé virtuální počítače jsou od sebe izolovány. [5]

Hyper-V používá Hypervisor jako tzv. mikrojádro, které obsahuje jen ty nejnutnější funkce pro virtualizaci. Jelikož jde o plně HW virtualizaci, je zapotřebí speciální HW s podporou virtualizace jako je AMD-V nebo Intel VT. Tato technologie pracuje pouze na architektuře x64bit. Toto se týká pouze hostujícího OS, jednotlivé virtuální počítače mohou být jak 64 bitové tak 32 bitové. Jako podporující hostované OS jsou Windows 2000 a novější. Zajímavostí je podpora některých OS Linux.

Existují dvě varianty, jakožto samostatný celek, nazýván Microsoft Hyper-V Server 2008 a jako role nacházející se v OS Windows. Samovolná varianta je zcela zdarma a obsahuje jádro systému Windows Server 2008 a to zahrnuje plnou funkcionalitu Hyper-V, avšak je limitována pouze na příkazovou řádku, jelikož neobsahuje GUI. Veškeré konfigurování se tedy provádí za pomocí shell příkazů a je možné spravovat i přes RDP, ale stále bez grafického rozhraní. [6]

Uplatnění této technologie je spíše ve firmách, které mají větší množství fyzických serverů zastávajících různé role. Díky této technologii je možno sloučit všechny fyzické servery do jednoho a tím ušetřit energii za provoz. K využití této technologie je zapotřebí již zmiňovaný speciální HW a také OS s podporou Hyper-V, poprvé ve verzi Windows server 2008. Také je podporován na osobních počítačích od verze OS Windows 8 Profesional, Enterprise a Educational, nelze jej použít na Home edici. U serverových OS Windows server 2008 a novější je ve verzích Standard, Enterprise a Datacenter.

Ovládání jednotlivých VM je velice jednoduché a lze je spravovat pomocí RDP nebo SSH. Existuje více možností, jak tuto službu nainstalovat, lze pomocí PowerShellu nebo na WS za pomocí správce serverů, kde vybereme možnost „Přidat role a funkce“ a s jednoduchým instalačním průvodcem dokončíme instalaci námi vybrané služby. U osobních počítačů je možnost instalace také přes Powershell, CMD nebo manuálně přes „Programy a funkce“, kde se nachází „Zapnout nebo vypnout funkce systému Windows“.

1.3 VPN – Virtual Private Network

Jedná se o propojení dvou bodů, které jsou realizované veřejnou či privátní sítí. Pro navázání spojení je potřeba ověřit totožnost stran za pomocí digitálních certifikátů a tím dochází k autentizaci. Tento způsob propojení se považuje za bezpečné, jelikož veškerá komunikace je šifrována. Uplatnění má jak, v hlasových tak datových sítích.

V mnoha případech se využívá pro připojení z veřejné sítě do intranetu firmy a díky tomu se uživatel choval, jako kdyby se nacházel přímo připojen do lokální sítě firmy, a to umožňuje vzdálenou správu. K tomu je zapotřebí na firemním serveru zprovoznit VPN server připojený do internetu, ke kterému se poté připojují VPN klienti odkudkoliv. VPN server plní funkci síťové brány, která zprostředkovává připojení a zabezpečuje veškerou komunikaci. Také je možné propojení více poboček dané firmy nezávisle na lokalitě a tím umožnit vzájemnou komunikaci. [7]

1.4 RDP – Remote Desktop Protokol

Je síťový protokol, vytvořený firmou Microsoft, umožňující uživateli vzdálené ovládání počítače pomocí připojení k jeho desktopovému prostředí. Funguje na principu klient-server, kdy uživatel za pomocí klienta se připojí na spuštěné GUI vzdáleného počítače. Je nutné dodat, že neumožňuje současnou práci více uživatelů.

Poprvé se objevil v OS Windows NT4.0 Terminal Server Edition. Existuje mnoho klientů pro připojení pomocí RDP na většinu verzí Windows, Mac OS X a jiných operačních systémů. Server implicitně používá TCP port 3389. Přímo od firmy Microsoft je nabízen klientský SW Remote Desktop Connection nebo Terminal Services Client. V dnešní době je vcelku populární také Teamwiever, který se dá použít jakožto vzdálené ovládání nebo v režimu Schůzka, který slouží pro různé prezentace a videohovory.

RDP využívá barevnou hloubku do 32bitů a také používá 128bitové šifrování algoritmem RC4, který je používán například pro šifrovaný přenos webových stránek nebo pro zabezpečený přenos v bezdrátových sítích. Podporuje funkci Audio redirection sloužící pro přesměrování výstupu zvuku ze vzdáleného počítače na lokální. Podobně pracuje funkce File System redirection, která umožňuje použít lokální soubor na klientovi na vzdáleném počítači a stejně tak existuje ještě funkce Printer redirection, která, umožňuje použít lokální tiskárnu pro tisk výstupů spuštěných programů na vzdáleném počítači. Dále umožňuje sdílenou schránku pro kopírování textu mezi lokálním a vzdáleným počítačem. Ve verzi 6.0 byla přidána další rozšíření jako je Remote programs, zabývající se spuštěním programu na vzdáleném počítači se soubory umístěnými na lokálním, a také Seamless windows, což je funkce umožňující spuštění vzdálených aplikací na straně klienta, jako by byly spuštěny lokálně. Jedna z dalších podstatných přidaných funkcí je Terminal server gateway, která slouží pro připojení prostřednictvím portu 443. [8]

1.5 NAS

NAS je zkratka pro Network Attached Storage, což je datové uložiště připojené v místní síti LAN. Ovšem nemusí plnit pouze funkci jakožto souborový server, ale například také jako klient sítě P2P, web server nebo také jako jednoduchý email poskytující uložiště. NAS servery obsahují vestavěný počítač, který plní funkce sdílení dat a podporu protokolů jako je NFS, SMB/CIFS nebo AFP. Obsahují jeden nebo více pevných disků, které jsou často uspořádány do logických, redundantních kontejnerů nebo jako RAID, což je metoda virtualizace, kdy dochází ke spojení dvou a více fyzických disků do jednoho uceleného logického svazku, který se poté tváří jako jeden pevný disk. [9]

Pro tyto servery jsou distribuovány OS Linuxu a FreeBSD jako jsou například FreeNAS, CryptoNAS, NASLite a mnoho dalších. Všechny tyto systémy jsou tvořeny tak, aby bylo snadné nakonfigurovat vše potřebné pro běh serveru a většina k tomu používá webový prohlížeč.

Konkrétně jsem pracoval se zařízením ReadyNAS 104 od firmy NetGear, který je určený spíše pro domácí využití, ale lze ho využít i pro firemní účely. Obsahuje procesor Marvell Armada 370 s frekvencí 1.2GHz, paměť o velikosti 512 MB, čtyři sloty na pevné disky typu SATA i SSD velikosti 2.5“ nebo 3.5“ s maximální kapacitou 16TB. Podporuje funkci Hot-swap, která umožňuje připojení či odpojení disků za chodu serveru. Dále obsahuje dva Gigabit LAN porty a tři USB porty z toho jeden verze 2 a zbylé verze 3. Fyzická podoba tohoto serveru je ukázána na následujícím obrázku. [10]

Obrázek 1.1: *Fyzická podoba ReadyNAS 104*

1.6 Server Message Block

Je síťový komunikační protokol na aplikační vrstvě ISO/OSI modelu, který se využívá pro sdílení přístupu k souborům, tiskárnám, sériovým portům a jiné komunikaci mezi uzly sítě. Také poskytuje mechanismus IPC, známý jako mezi-procesová komunikace, která slouží pro výměnu dat mezi dvěma nebo více procesy či vlákny.

Tento protokol pracuje v lokálních sítích na principu klient-server, kdy klient si zažádá o přístup a server na to odpoví. Server povoluje přístup ke sdíleným prostředkům klientovi jako jsou sdílené disky, adresáře nebo tiskárny. Veškerá komunikace probíhá výměnou paketů SMB, kde Server přijímá a vyhodnocuje, zda má klient přístupová práva a poté zahajuje požadovanou operaci s odesláním výsledku zpět klientovi identickým paketem SMB. Spojení běží přímo na TCP portu 445 nebo pomocí NetBIOS API na portech TCP 137, 139 a UDP 137, 138. V následující tabulce je ukázán formát paketu SMB. [11]

Tabulka 1.3: *Paketová hlavička protokolu SMB*

	SID	S	C	RC	AH	RC	RS	NID	PID	UID	MID	P	PCd	BL	B
Byte	1	3	1	1	1	2	15	2	2	2	2	1	2	2	1

Tabulka 1.4: *Popis paketové hlavičky protokolu SMB*

Označení		Význam
SID	SMB Identification	Identifikace protokolu SMB (0FFh)
S	Server	Identifikace dialektu serveru SMB
C	Command	Funkční kód volané služby SMB
R	Return Class	Třída návratového kódu funkce SMB
AH	Ahregister procesoru	Výsledek operace v registru AH procesoru
RC	Return Code	Návratový kód operace
RS	Reserve	Rezerva pro budoucí rozšíření
NID	Net Path ID	Identifikátor přiřazený sdílenému prostředku
PID	Process ID	Identifikátor procesu klienta
UID	User ID	Identifikace uživatele
MID	Multiplex ID	Multiplexní identifikátor procesu klienta
Prmct	Parameter Count	Počet volitelných parametrů k volané funkci
PC	Parameter Code	Kód parametru volané funkce
BL	Buffer Length	Délka datové části SMB bloku
B	Buffer	První slabika datové části bloku SMB

Existují dvě metody přístupu ke sdíleným prostředkům z pohledu serveru. První metoda je přístup pomocí hesla přiřazeného přímo k danému sdílenému prostředku, kdy, po zadání správného hesla, se klientovi přidělí NID. Druhá metoda používá ověření uživatelským jménem a heslem, kdy, v případě správnosti, bude klientovi přiřazen uživatelský identifikátor, pomocí něhož server ví, jaká má klient přístupová práva.

2 RADIUS server

Jedná se o protokol autentizace, autorizace a účtování, který se používá pro přístup k síti nebo IP mobilitu, jak lokálně, tak i v roamingu. Nejdůležitějším prvkem je vysoká síťová bezpečnost, jelikož transakce mezi klientem a RADIUS serverem je autentizována pomocí takzvaného sdíleného tajného klíče, který není nikdy poslán přes síť. [12]

2.1 Vytvoření virtuálního počítače

Nejdříve bylo zapotřebí připojit se na firemní server, na kterém běží virtuální jednotky. Připojil jsem se pomocí RDP jako administrátor, abych měl dostatečná práva na požadovanou práci. Po přihlášení do serveru jsem spustil program Hyper-V, kde se nacházejí již funkční virtuální jednotky. Bylo zapotřebí vytvořit nový virtuální počítač, který poté byl připojen do firemní domény a slouží jakožto RADIUS server. Ve správci technologie Hyper-V jsem tedy vybral možnost „přidání nového VM“ a tím se otevřel instalační průvodce, kde se nejdříve musel zadat název VM, jelikož se používá ve firmě daná politika jmen, tak byl pojmenován jako dc, jakožto třetí doménový řadič ve firmě. Dále je na výběr generace VM. Rozdíl mezi první a druhou generací je ten, že druhá generace má založený firmware na rozhraní UEFI a tím pádem podporuje pouze 64 bitové verze operačních systémů, zatímco první generace podporuje i systémy 32 bitové. Po vytvoření VM nelze již měnit generaci. Poté bylo nutno přidělit paměť v jednotkách MB. Byla zvolena velikost 4096 MB, aby měl DC dostatečnou kapacitu. Zde je možné využití dynamické paměti, to znamená, že používá tolik paměti, kolik potřebuje a zbytek z velikosti je tedy dostupný i pro ostatní VM fyzického serveru. Následující krok se týká konfigurace sítě, kde každý virtuální počítač obsahuje síťový adaptér, který je možno nakonfigurovat tak, aby používal virtuální přepínač, nebo může zůstat odpojen. Předposledním krokem je připojení virtuálního pevného disku. Na výběr jsou tři možnosti, vytvořit nový, použít již existující virtuální disk nebo připojit později. U vytváření nového je zapotřebí určit název, umístění, kde se bude nacházet a velikost maximálně 64 TB. Když použijeme možnost připojení existujícího virtuálního disku, tak je zapotřebí, aby byl ve formátu VHD nebo VHDX a také cestu kde je umístěn. Posledním krokem je vybrání možnosti instalace OS, kde je na výběr možnost instalace později, ze spouštěcího CD či DVD pomocí bitové kopie ISO, pomocí virtuální spouštěcí diskety VFD nebo z instalačního serveru v síti. Pokud je vše vybráno podle potřeb, lze přejít ke shrnutí a potvrzení vytvoření nové VM.

2.2 Instalace OS

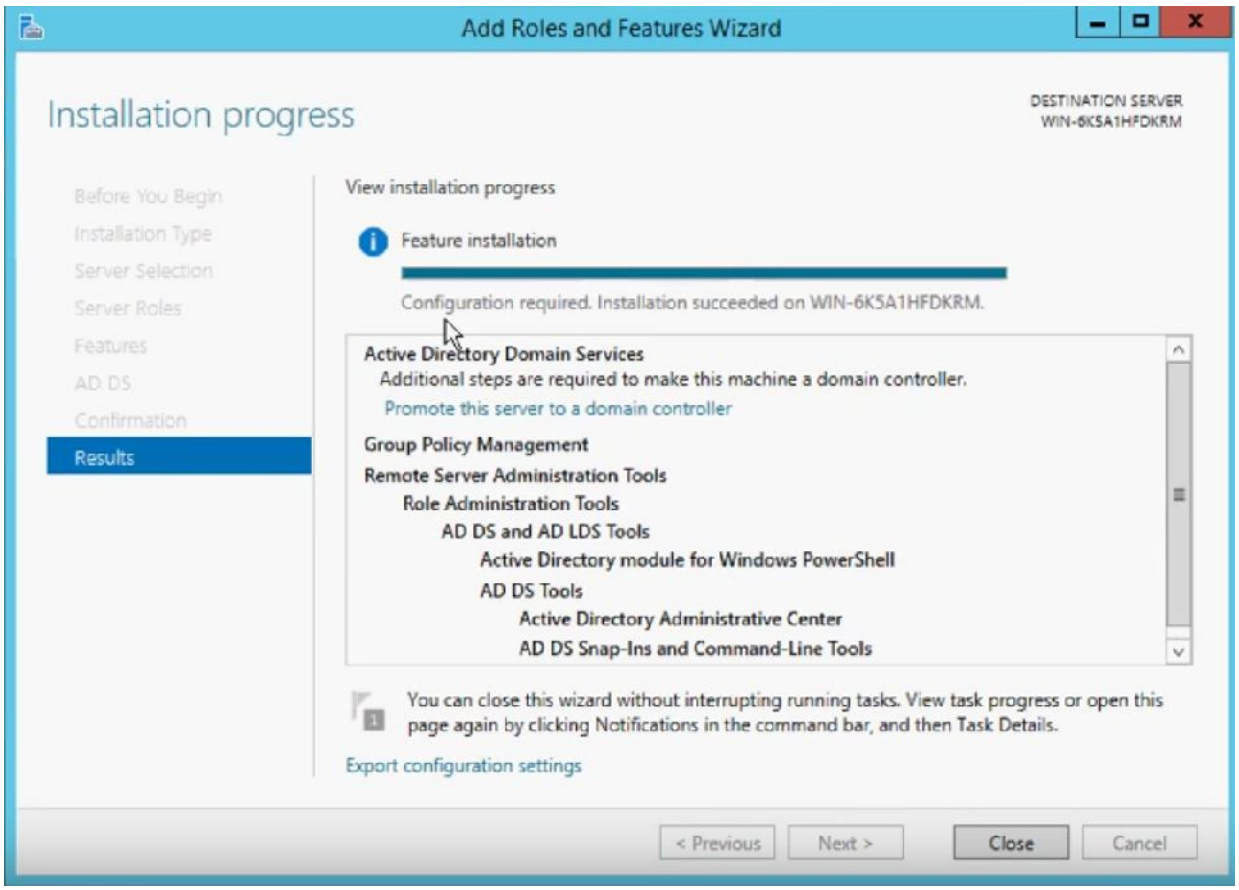
Jak již bylo zmíněno, je zapotřebí nainstalovat na nově vytvořený virtuální počítač vhodný OS. Firma získala licenci na nově uvolněnou verzi OS Windows server 2016, tak jsem použil ji. Jelikož jsem při vytváření virtuálního počítače zvolil možnost instalace OS později, bylo zapotřebí v nastavení daného virtuálního počítače přidělit médium s bitovou kopií OS, která je umístěna na fyzickém serveru firmy. Po přidělení média je potřeba virtuální počítač spustit a připojit se k němu. Poté instalace probíhá v podstatě stejně jako u desktopových verzí. Je jen nutné vybrat verzi s GUI nebo pouze Nano, o které jsem se zmínil ve druhé kapitole a která se používá převážně pro cloudové aplikace. Tento server je využíván k provozu helpdesku, takže bylo zapotřebí zvolit verzi s grafickým rozhraním. Po úspěšné instalaci následovala konfigurace serveru pro připojení do firemní domény a následná implementace služeb pro zprovoznění RADIUS serveru.

2.3 Služba AD DS

Tento server bylo nutno připojit do firemní domény a toho jsem dosáhl pomocí služby Active directory Domain Services, která slouží pro škálovatelnost, bezpečnost a ovládání infrastruktury pro uživatele a správce. V Server manageru jsem vybral „přidat role a služby“ a tím se spustil instalační průvodce, kde jako první bylo potřeba vybrat, zda chceme role a služby instalovat na fyzickém počítači či virtuálním nebo na vypnutém virtuálním disku. Jelikož jsem potřeboval nainstalovat AD DS na lokálním serveru, tak jsem v další nabídce nechal vybraný lokální server a pokračoval na výběr potřebné služby. Pokud není požadováno instalovat něco dalšího, co by měl server potřebovat, stačí následující okna proklikat na potvrzující stránku, kde je možnost automatického restartování serveru po nainstalování služby.

2.3.1 Doménový řadič

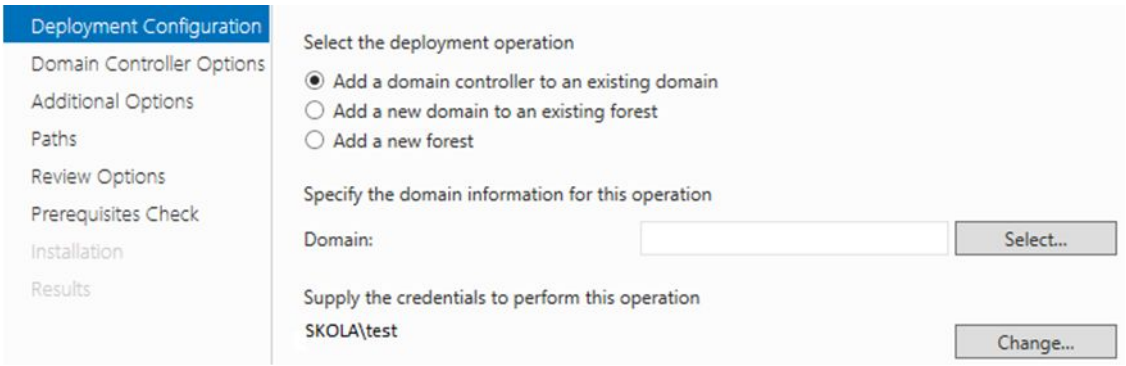
Jakmile se nainstaluje služba AD DS, je zapotřebí, aby se ze serveru stal doménový řadič, který má za úkol odpovídat na bezpečnostní autorizační požadavky, jako je přihlášení nebo kontrola práv uvnitř domény. Existuje více způsobů, jak otevřít nastavení pro doménový řadič. Na konci instalace na stránce result se nachází aktivní odkaz pro povýšení serveru na doménový řadič nebo, pokud byla zvolena možnost automatického restartování, lze pomocí Server manageru v upozorněních vybrat možnost povýšení viz Obrázek 2.1.



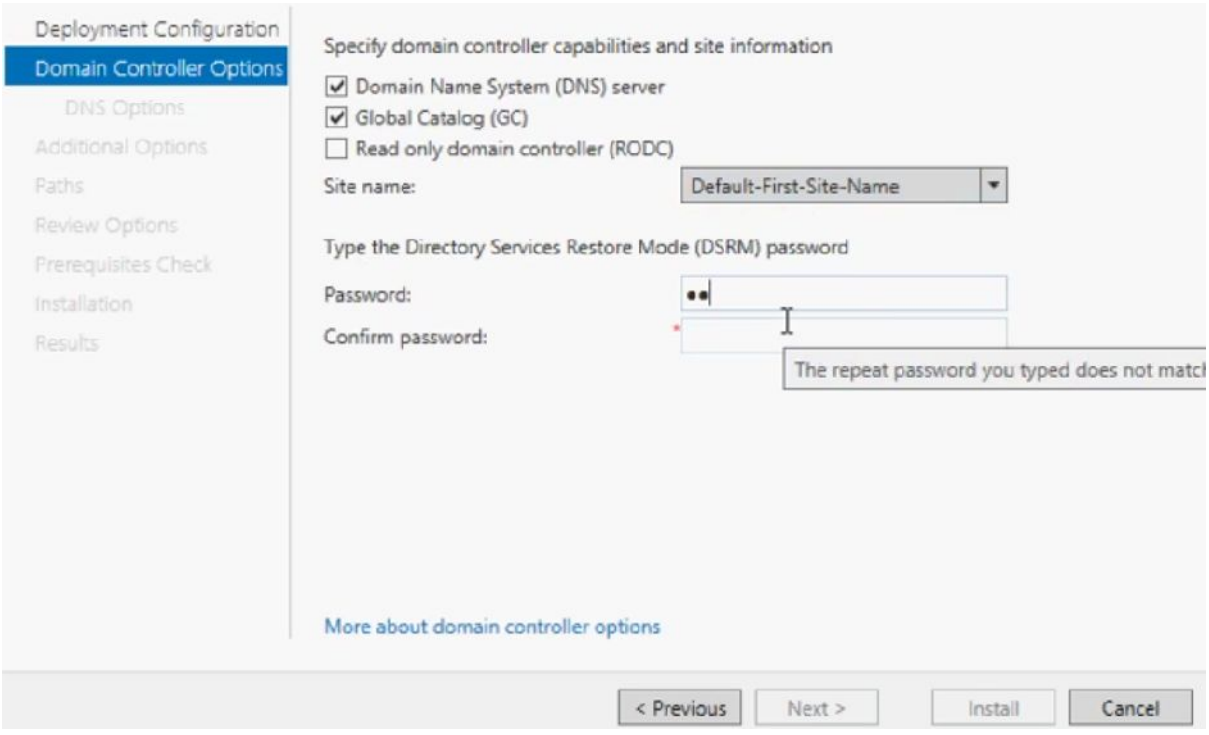
Obrázek 2.1: *Povýšení serveru na DC na konci instalace*

2.3.2 Nastavení DC

Jelikož firemní doména již existuje, zvolil jsem možnost přidání doménového řadiče do existující domény. Dále bylo zapotřebí zadat jméno domény, do které jsem se chtěl připojit, a to vyžadovalo autorizovaného uživatele s přístupem do domény viz Obrázek 2.2. Po úspěšném ověření následovala specifikace doménového řadiče, zda bude DNS, GC nebo bude jen ke čtení. Global Catalog obsahuje sadu všech objektů v AD DS a je řadičem, jenž ukládá úplné kopie všech objektů v adresáři hostitelské domény a částečné kopie, které jsou jen pro čtení. Možnost pouze ke čtení se používá v případě, pokud není zaručena bezpečnost serveru a pokud víme, že se z něho nebude nic měnit v AD. Veškeré nastavení AD získává z nadřazených serverů v doméně. V mém případě jsem server použil jako DNS a GC viz Obrázek 2.3. Dále bylo zapotřebí zadat heslo pro obnovení a následovalo nastavení DNS, které se nastavilo později. V další fázi bylo nutné nastavit, kde se bude nacházet databáze AD DS, log soubory a SYSVOL. Poslední krok byl pouze pro ověření před potvrzením instalace. Jakmile proběhla instalace v pořádku, systém se automaticky restartoval a poté již vyžadoval přihlášení uživatele z domény.



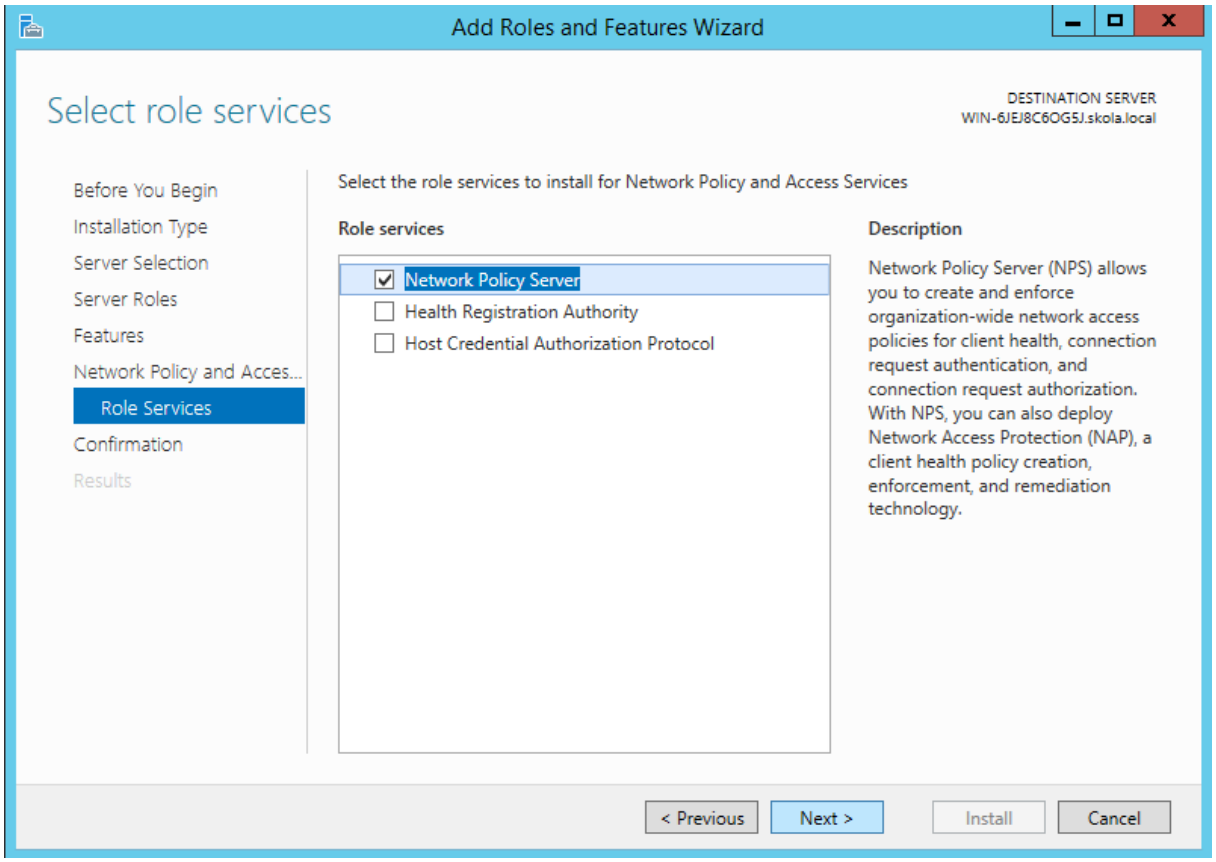
Obrázek 2.2: *Přidání DC do domény*



Obrázek 2.3: *Specifikace rolí DC*

2.4 Služba „Síťové zásady a přístup“

Pro zprovoznění RADIUS serveru bylo zapotřebí nainstalovat serverovou službu Síťových zásad a přístupů viz Obrázek 2.4. Může fungovat jakožto Server NPS, služba Směrování a vzdálený přístup, Autorita pro registraci stavu a také protokol HCAP. NPS server umožňuje spravovat přístup k síti prostřednictvím různých serverů pro přístup k síti jako jsou bezdrátové AP, servery VPN, servery pro telefonické připojení a ověřovací přepínače 802.11X. NPS lze také použít k zabezpečenému ověřování hesla protokolem PEAP u bezdrátových připojení nebo pro nasazení architektury NAP v síti.



Obrázek 2.4: *Instalace Síťových zásad*

Při instalaci služby síťových zásad a přístupu bylo nutno vybrat roli NPS. K tomu, aby vše fungovalo bylo zapotřebí nainstalovat službu AD CS.

2.4.1 **AD CS**

Slouží pro správu a vydání certifikátů v systémech softwarového zabezpečení, které používají technologie veřejných klíčů. V tomto případě stačilo vybrat roli pro správu CA, u které v dalším kroku bylo zapotřebí vybrat volbu Enterprise, aby mohla využívat data z AD k usnadnění správy certifikátů. Dále následovalo vybrání typu CA. Na výběr bylo ze dvou možností. První možností byla root, která se vybírá v případě, že bude jediný CA v infrastruktuře veřejných klíčů. Druhou možností byla subordinate, která se využívá tehdy, jestliže se v doméně nachází nějaká infrastruktura veřejných klíčů a tuto chceme přiřadit jako podřízenou. Jelikož to byla první instalace CA v doméně, zvolil jsem první možnost. V dalším kroku následovalo vytvoření nebo použití již existujícího privátního klíče. Neboť jsem neměl k dispozici existující privátní klíč, musel jsem vytvořit nový. K jeho vytvoření v následujícím kroku bylo nutno zvolit kryptografii, ve které se volí zprostředkovatel kryptografických služeb, hash algoritmus a délka klíče. Zprostředkovatele jsem nechal původně vybraného, kterým je RSA#Microsoft Software Key Storage Provider. Dále jsem vybral délku 2048 znaků a hash algoritmus SHA1. Dále následovalo pojmenování a délka platnosti privátního klíče. Jméno jsem zanechal původně vygenerované a platnost na pět let. Posledním krokem byl výběr umístění databáze certifikátů, která je původně v systémové složce system32.

2.4.2 **Konfigurace RADIUS serveru**

Další v pořadí byla již samotná konfigurace RADIUS serveru, která se nachází ve službě síťových zásad. Po otevření této služby bylo potřeba registrovat server do AD Za pomoci konfiguračního průvodce se vybírá typ, kterou z funkcí chceme nastavit. Na výběr je ze tří možností, první NAP, druhá RADIUS server pro vytáčení nebo VPN a třetí je RADIUS server pro 802.1x bezdrátové nebo drátové připojení. Jelikož bylo vyžadováno, aby RADIUS server fungoval pro bezdrátovou firemní síť, zvolil jsem možnost „Zabezpečené bezdrátové připojení“ a pojmenoval ho Wireless. Dále následovalo nastavení klienta, kde bylo potřeba zadat jméno, IP nebo DNS a nejdůležitější sdílený klíč. V dalším kroku bylo vybrání typu autentizace, kde bylo možno vybrat Smart Card nebo jiné certifikáty, PEAP anebo Zabezpečené heslo EAP-MSCHAP v2. Zvolil jsem jednu z uvedených možnost a později jsem přes síťové politiky přidal ještě metodu EAP-MSCHAP v2. Posledním důležitý krokem bylo nastavení skupiny uživatelů, kteří mají mít přístup do firemní bezdrátové sítě. Protože nebyly žádné specifické požadavky, aby někdo nemohl mít přístup, zvolil jsem skupinu Domain Users. Aby vše fungovalo, bylo zapotřebí ještě nastavit zabezpečení na AP Cisco Meraki, kde bylo potřeba zadat IP adresu a port RADIUS serveru, typ šifrování a sdílený tajný klíč.

3 Helpdesk

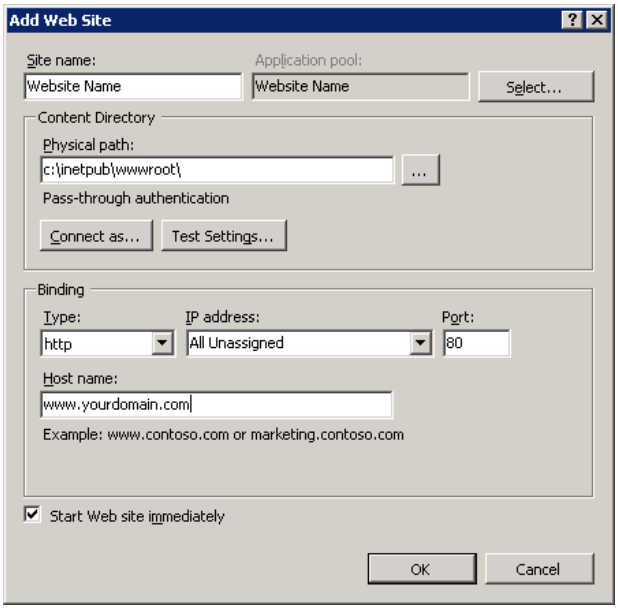
Po úspěšné implementaci RADIUS serveru jsem dostal za úkol na firemním serveru zprovoznit Helpdesk systém pro zpracovávání a vyřizování klientských požadavků. K tomuto účelu jsme po konzultaci vybrali systém osTicket, který je volně dostupný a je psaný jazykem PHP.

Jelikož se ve firmě používá WS, tak instalace osTicketu proběhla pomocí služby Webový server neboli IIS, která poskytuje bezpečnou, modulární a rozšiřitelnou platformu pro hostování webových stránek, služeb a aplikací. Umožňuje sdílení s uživateli v intranetu nebo extranetu. IIS je webová platforma, která integruje služby ASP.NET, FTP, jazyk PHP a technologii WCF.

V základní verzi IIS se nenachází podpora PHP jazyka, a proto bylo potřeba ji doinstalovat pomocí Web platform installer, který je také doinstalovanou službou v IIS. Pro podporu osTicket se vybrala verze PHP 7.0 a pro databázi MYSQL 5.5.

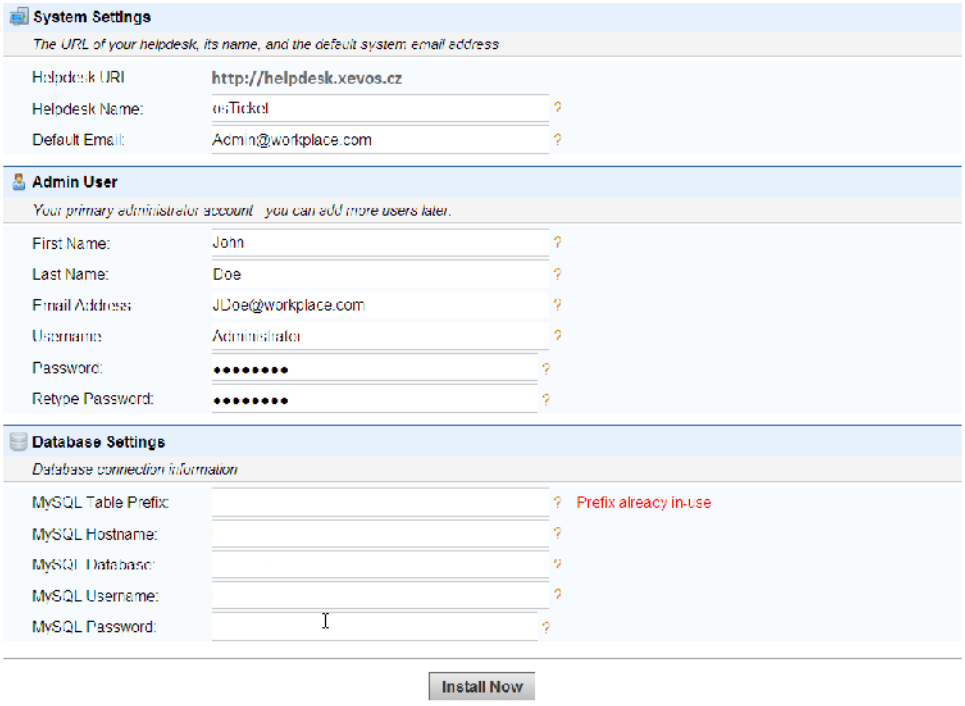
3.1 Instalace osTicket

V IIS bylo potřeba přidat novou stránku se jménem helpdesk, fyzickou cestu k tomuto systému, která se nachází na disku C. Dále se zadává IP adresa pro přístup z lokální sítě a hostující jméno, které je konkrétně helpdesk.xevos.cz viz Obrázek 3.1.



Obrázek 3.1: *Přidání nové stánky do IIS*

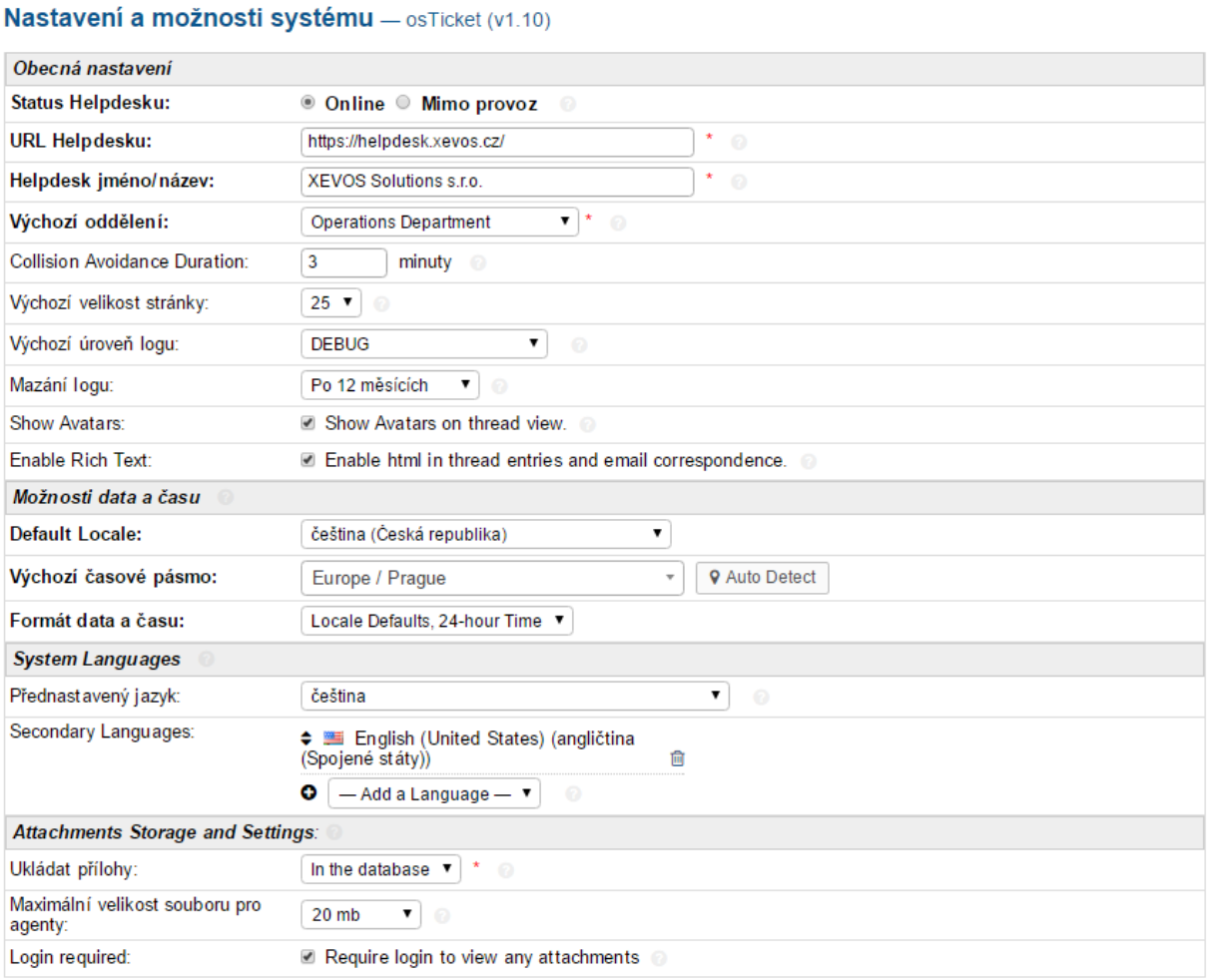
Následovala již samotná instalace osTicketu, kde bylo zapotřebí zadat název, defaultní email, administrátorského uživatele a nastavení databáze. Poté byl nahrán firemní design a začal jsem nastavovat vnitřní funkce systému viz Obrázek 3.2.



Obrázek 3.2: *Instalace osTicket*

3.2 Konfigurace osTicket

Jako první bylo nastavení základních funkcí osTicketu jako je obecné nastavení, možnosti datumu a času, systémový jazyk a nastavení pro přílohy viz Obrázek 3.3. V obecném nastavení jsou povinné parametry jako status helpdesku, zda je vypnutý či zapnutý, URL, název a výchozí oddělení. Dále obsahuje vyhnutí kolize, výchozí počet záznamů na stránce, úroveň log souboru a dobu jeho mazání, zobrazení uživatelských avataru a podporu RTF. V nastavení datumu a času se určuje poloha serveru, výchozí časové pásmo a časový formát. Poslední část se týká nastavení příloh, kam se mají ukládat, jakou maximální velikost mohou mít a zda je potřeba být přihlášen pro jejich zobrazení. Jelikož byla nastavena maximální velikost pro přílohy 2 MB, což bylo nedostačující, musel jsem nalézt, kde se dá tato možnost zvětšit. Zjistil jsem, že toto nastavení se týká přímo PHP manageru a jeho souboru php.ini, ve kterém bylo potřeba změnit atribut upload_max_filesize na požadovaných 20 MB.



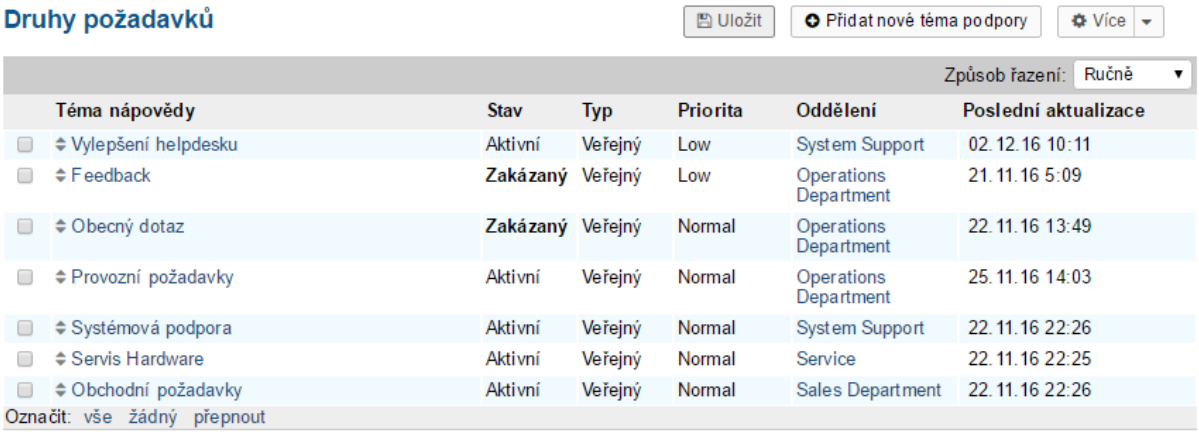
Obrázek 3.3: *Konfigurace systému osTicket*

Dále bylo nutné přidat výchozí stránky jako je vstupní, mimo provoz a děkovná. Přidání a jejich následné upravování se nachází v záložce spravovat, kde je formulář stránek a plno dalších funkcí tohoto systému. Při jejich vytváření se musí zadat název, typ, stav a text na stránce.

3.2.1 Nastavení požadavků

Jelikož se jedná o Helpdesk, bylo potřeba nastavit nejzákladnější funkci, kterou jsou požadavky neboli tickety. Ve výchozím nastavení bylo potřeba určit výchozí formát čísla ticketu, který je IR17#####. Dále bylo nutno určit výchozí stav jako otevřený, prioritu normální a SLA standardní, které je 72 hodin a označuje smlouvu sjednanou mezi poskytovatelem služby a jejím uživatelem. Další podstatnou možností bylo zapnout verifikaci člověka, aby nikdo nemohl zahltit systém požadavky.

Následně bylo potřeba vytvořit druhy požadavků, do kterých se později nahrály potřebné formuláře, a vytvořit možnosti SLA viz Obrázek 3.4.



Obrázek 3.4: *Druhy požadavků*

Při vytváření nového druhu požadavku je potřeba nastavit téma, stav, typ a jestli se jedná o podřazené nebo téma nejvyšší úrovně, také lze přidat interní poznámku. Dále se při vytváření nastavuje, kterému oddělení se mají tyto požadavky přidělovat, číselné označení, stav, priorita, SLA a odkaz na stránku s poděkováním. Je také možnost přímo určit agenta, kterému budou dané požadavky přidělovány. V posledním kroku se přidávají volitelné formuláře, které se k danému tématu musejí nejdříve vytvořit.

3.2.2 Volitelné formuláře

Obsahují veškeré důležité informace o požadavku od uživatele, aby agenti mohli co nejlépe vyřešit daný problém. Nachází se v administrátorském panelu v sekci Spravovat, kde je přehled vestavěných a volitelných formulářů.

U vytváření nových volitelných formulářů se musí zadat název a vytvořit pole prvků, která se budou nacházet ve vybraném tématu. Pole prvků obsahuje název prvku, typ, viditelnost a proměnnou. Podle toho, jaký se zvolí typ, bude následná konfigurace, kde pro všechny je stejná část, zda bude prvek povolen, povinný, viditelný a upravitelný. Pokud se jednalo o krátkou odpověď, nastavila se maximální velikost. U typu Volby bylo potřeba zadat pole prvků, ze kterého uživatel bude vybírat možnosti, a zda je možnost výběru více možností. Další důležitý typ je Nahrání souboru, u kterého lze omezit velikost, jakého typu budou přílohy a maximální počet příloh. Existují další typy jako je telefonní číslo, datum a čas, dlouhá odpověď, zaškrtávací pole a další. Na následujícím Obrázku 3.5 je příklad, jak jsem vytvářel formulář pro HW údržbu. Povinnými atributy jsou model zařízení a údaj o tom, zda je v záruce, ostatní jsou volitelná.

***Pole formuláře** pole jsou dostupná tam, kde je tento formulář použit*

Popis	Typ		Viditelnost	Proměnná	Smazat
Druh zařízení	Volby	Konfigurace	Volitelné		
Značka	Volby	Konfigurace	Volitelné		
Název zařízení (model)	Krátká odpověď	Konfigurace	Vyžadováno		
P/N	Krátká odpověď	Konfigurace	Volitelné		
Serial Number	Krátká odpověď	Konfigurace	Volitelné		
Příloha	Nahrání souboru	Konfigurace	Volitelné		
Zařízení v záruce?	Volby	Konfigurace	Vyžadováno		
+	Krátká odpověď		Volitelné		

Obrázek 3.5: *Volitelný formulář HW údržby*

3.2.3 Plány SLA

Jak již bylo zmíněno, v dalším kroku jsem vytvořil jednotlivé SLA, které slouží pro určení priority zpracování požadavků. Při jejich vytváření je nejdůležitějším atributem bezúročné období, které stanoví počet hodin, po kterých je vytvořený ticket označený jako zpožděný. Standardně je nastaveno 72 hodin od vytvoření ticketu. Měl jsem za úkol vytvořit pět intervalů a to po 2, 4,6, 24 a 48 hodinách viz Obrázek 3.6. Dále, aby měly nějaký význam, bylo nutno přidat jednotlivé intervaly do filtrů požadavků.

Přidat nový plán SLA

Požadavky jsou označeny jako meškající po uplynutí nastavené doby.

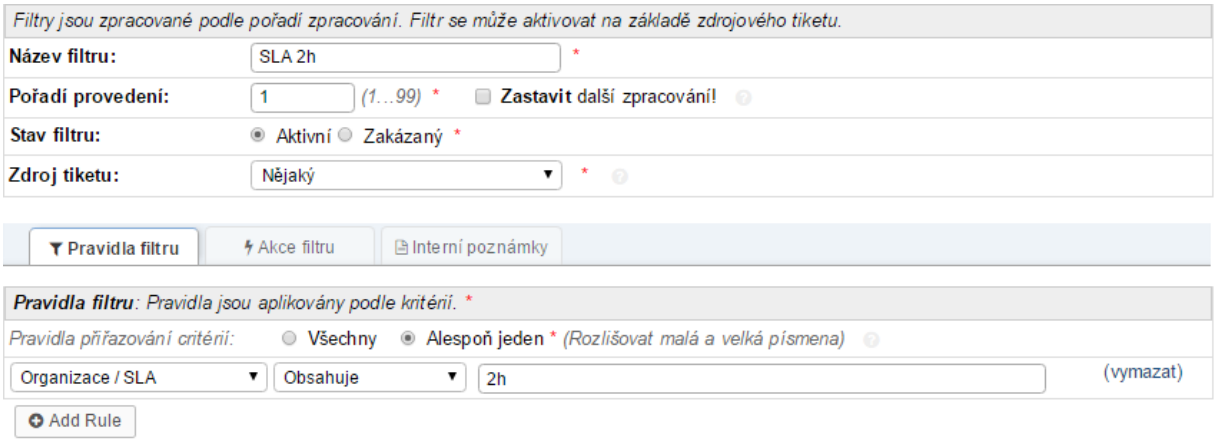
Jméno:	2h *
Bezúročné období:	2 *(v hodinách)* *
Stav:	**Aktivní** Zakázaný *
Přechodné:	SLA může být přepsáno při přeposlání tiketu nebo změně tématu podpory
Upozornění na meškající požadavky:	**Zakázat** upozornění na meškající požadavky. *(Přepíše globální nastavení)*

Obrázek 3.6: *Přidání nového plánu SLA*

3.2.4 Filtry požadavků

Zde se vytvářejí filtry, které mají za úkol určit pořadí, ve kterém se budou jednotlivé tickety vyřizovat. Hlavním pravidlem pro tyto filtry je hodnota smluv SLA, kdy nejnižší, 2 hodinová, má nejvyšší prioritu a standardní SLA, která je 72 hodin, má nejnižší. Samozřejmě se dají tyto filtry použít mnoha dalšími způsoby, jako je například přiřazení týmu či agenta, nastavení závažnosti, odmítnutí tiketu a další.

Bylo potřeba vytvořit filtr pro každý SLA plán, které jsem vytvořil v předchozím kroku. Jednotlivé filtry mohou obsahovat více pravidel. V mém případě bylo potřeba pouze jedno, a to podle hodnoty SLA dané organizace viz Obrázek 3.7. Příkladem je SLA pro dvě hodiny, kdy pořadí provedení je nejvyšší možné, stav filtru aktivní a zdroj ticketu nějaký, jelikož není podporována jiná možnost než pomocí webového formuláře. Aby byl filtr splněn, je potřeba určit, zda musí být všechna pravidla splněna, nebo stačí alespoň jedno. Akce samotného filtru, co má vykonat, se nachází na další záložce, kde v mém případě bylo potřeba vybrat plán SLA pro dvě hodiny.



Obrázek 3.7: *Vytvoření nového filtru požadavků*

3.2.5 Vytvoření Agentů

K celkovému fungování tohoto systému také patří agenti neboli zaměstnanci firmy, kteří vyřizují požadavky zákazníků a interní požadavky firmy. Každému zaměstnanci byl vytvořen účet, kterým se přihlašuje do systému rolí agenta a může tak zpracovávat zadané požadavky. Aby se agenti dostali do systému, musí se přihlásit přes přihlášení určené přímo pro agenty.

Při vytváření nového agenta je potřeba nastavit uživatelské jméno a heslo. Další důležitou součástí je nastavení oddělení, ve kterém bude daný agent pracovat a přístup, zda bude mít plný nebo omezený. Na další záložce se nachází oprávnění na správu uživatelů a organizací. Posledním krokem před vytvořením je vybrání týmu, do kterého bude agent přiřazen. Ve firmě jsou čtyři týmy.

4 Implementace GPO

Jedním z mých dalších úkolů bylo vytvoření různých pravidel pro klientský server. Pravidla měla přidělovat práva daným skupinám uživatelů. Jelikož se server nenacházel přímo v místě pracoviště, bylo potřeba se připojit do interní sítě klienta pomocí VPN. Konkrétně jsem k tomu využil Open VPN program, do kterého je potřeba vložit konfigurační soubor s potvrzenými certifikáty. Po úspěšném napojení do sítě jsem využil pro přímé připojení k serveru službu RDP, která je automaticky vestavěná jako základní funkce systému Windows.

4.1 Vytvoření skupin

Než jsem mohl vytvořit jednotlivé GPO, bylo potřeba rozdělit uživatele do skupin podle přidělených práv. Veškeré vytváření a úpravy probíhají ve službě AD Users and Computers. Potřeboval jsem vytvořit dvě základní skupiny pro uživatele, a to Server Admins a Desktop Admins. Dále bylo potřeba rozdělit serverové počítače od klientských desktopů, a to podobným způsobem jako u uživatelů, ale jelikož byly všechny vloženy do jedné skupiny, měl jsem na výběr, pro které počítače vytvořím vlastní skupinu. Vybral jsem skupinu pro desktopové, které jsem tedy odebral z předchozí skupiny a přidělil je do nově vytvořené Domain Desktops.

4.2 Vytvoření GPO

Český překlad je Skupinové politiky, které slouží pro nastavení chování systému pro uživatele a jednotlivé počítače. Mohou být pouze lokální, na úrovni celé domény, pro danou organizační jednotku nebo také pro stránky provozované na daném serveru. Je možno využít již automaticky vytvořenou GPO pro doménu, ale pro větší přehled je lepší vytvořit novou, kde budou jen potřebná pravidla. Vytvořil jsem tedy GPO na úrovni domény, aby se mohla aplikovat pravidla pro dané uživatele a počítače v celé firemní doméně. Do správy skupinových politik se dá dostat vícero způsoby, buď pomocí server managera nebo přes příkaz spustit, kde se zadá gpmc.msc. Následovala implementace GPO. Nejdříve jsem vytvořil nový objekt skupinových politik, ve kterém se nastavují potřebná pravidla, a nakonec je potřeba tento objekt připojit na doménu. Začal jsem GPO pro servery. Aby měly vytvořené skupiny určená práva na doménových serverech, bylo potřeba přidat je do Restricted Groups, kde je nutno nastavit, v jakých skupinách budou členy. Jelikož měly mít práva administrátora, přidělil jsem je do skupiny Administrators. Aby byl možný také vzdálený přístup, byly přiděleny rovněž do skupiny Remote Desktop Users. Poslední přidanou skupinou byla Domain Servers, aby se specifikovalo, na které počítače mají mít tato práva. Veškeré nastavení se nachází v Computer Configuration v podsložce Windows Settings, kde je složka Security Settings a v ní se nachází již potřebné Restricted Groups. Obdobně následovalo nastavení pro desktopy, ale zde bylo ještě potřeba zakázat vzdálené připojení pro skupinu externisté. Jak již bylo zmíněno, po nastavení je potřeba nové objekty GPO připojit na doménu, a to se provede pravým kliknutím na jméno domény a vybráním příkazu Link an Existing GPO. Ještě je potřeba aktualizovat politiky příkazem gpupdate v příkazové řádce cmd. Vše bylo nutné otestovat, což jsem provedl pomocí nově vytvořeného testovacího uživatele, kterého jsem podle potřeby přemisťoval do jednotlivých skupin.

5 Sdílení NAS serveru

Nakonec jsem připravoval pro klienta podle šablony sdílený síťový disk NAS serveru, na kterém bylo potřeba vytvořit složky a přidělit jim jednotlivá práva, kdo bude mít do těchto složek přístup a jaký. Tento server byl již připojen do firemní domény a díky tomu měl již importované všechny potřebné uživatelské účty z AD. Jelikož server byl fyzicky vzdálený, bylo potřeba zase použít VPN tentokrát vestavěnou od Microsoftu s typem L2TP/IPsec, kde je potřeba znát sdílený klíč, uživatelské jméno a heslo, kterým jsem se do vnitřní sítě napojil jako administrátor.

5.1 Vytvoření sdílených složek

Po připojení do sítě jsem se napojil na NAS server pomocí webového prohlížeče, jelikož má jednoduchou webovou podporu, kde se vše potřebné nastavuje. Existují i NAS servery bez webové podpory a ty je potřeba spravovat přes příkazovou řádku. Dále následovalo vytvoření složek a nastavení pomocí, které služby budou přenášeny. Jelikož se ve firmě pracuje se systémem Windows, byla vybrána služba SMB. NAS server podporuje i NFS, AFP, FTP a mnoho dalších. Při vytvoření je defaultně nastaven přístup pro všechny, a to i bez přihlášení, takže se jednalo o přístup anonymous. To bylo třeba změnit a nastavit primárně plný přístup pouze pro administrátora. Abych mohl přidělit práva a nastavit tak finální podobu, potřeboval jsem se připojit i na firemní server přes RDP, odkud jsem se poté přes správce souborů napojil na NAS server s administrátorským přihlášením.

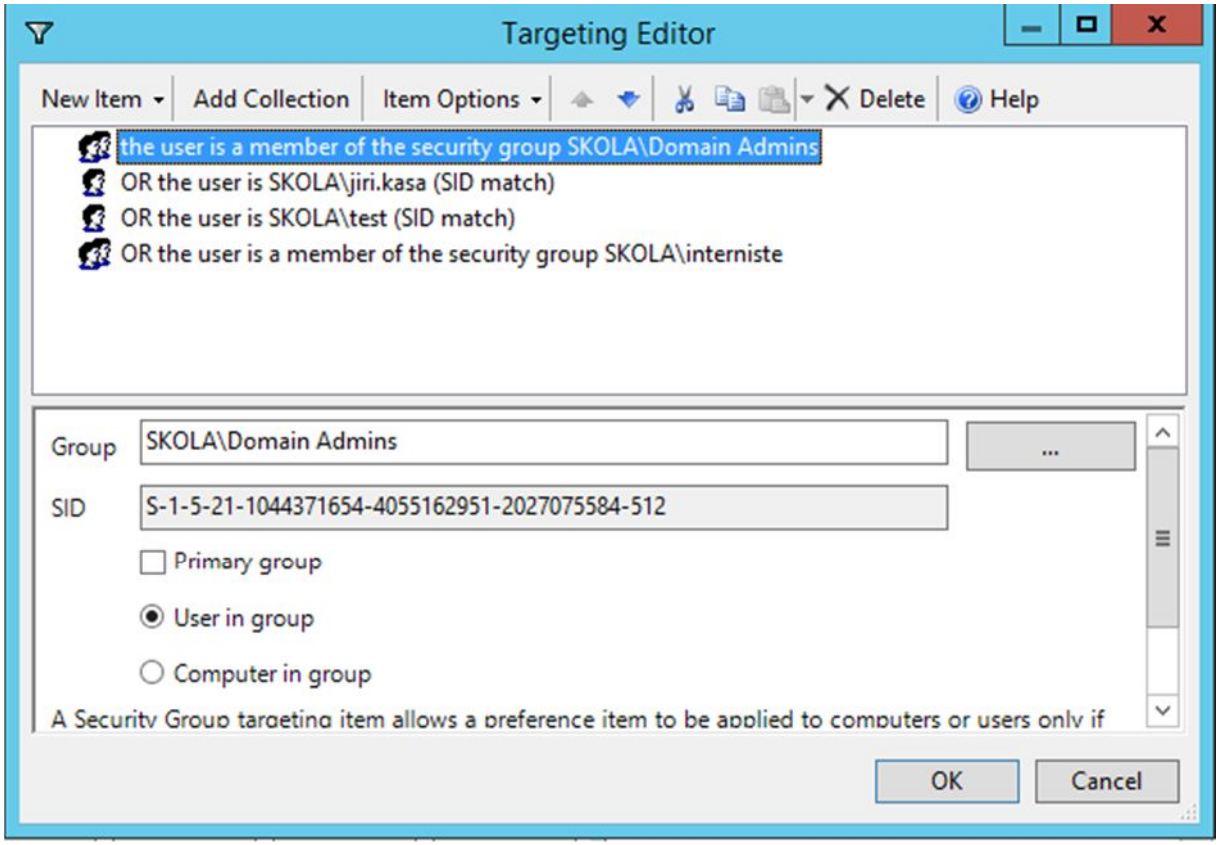
Vše fungovalo v pořádku do doby, než jsem chtěl změnit přístupová práva pro jednotlivé složky. Jelikož jsem byl přihlášen jako administrátor, měl jsem mít všechna práva, ale nebylo tomu tak. Z neznámého důvodu jsem neměl přístup do jednotlivých složek. Abych se do nich dostal, změnil jsem tedy přístup zpět na anonymous, díky kterému jsem mohl přidělit práva podle šablony. Po přidání uživatele z domény se naskytl další problém. Nepřeložil se SID, což je unikátní identifikátor pro uživatele nebo skupinu. Po mnoha hodinách hledání chyby a různém testování nastavení přístupu, jsem, po konzultaci s pracovníkem firmy, došel k závěru, že chyba je někde mezi NAS serverem a připojením do domény. Zkusil jsem tedy NAS server odpojit od domény a znovu připojit, jenže po připojení zpět se jevil jako neexistující, jelikož se sama vypla služba SMB. Když jsem se ji pokusil zapnout, zůstala ve stejném stavu. Pro vyřešení tohoto problému bylo poslední možností restartování NAS serveru, což není zrovna bezpečné řešení, jelikož se jednalo o vzdálený server. Kdyby nastala chyba při bootování, neměl bych možnost ji opravit. Po úspěšném restartu služba SMB naběhla a s tím i práva jednotlivých uživatelů.

5.1.1 Přidělení práv

Podle šablony bylo potřeba nastavit přístup do jednotlivých složek a jejich podsložek. Všechny mají primárně nastavenou neviditelnost a uvidí je pouze ti uživatelé, kteří k nim mají mít přístup. Například složka ÚČETNICTVÍ obsahuje další tři podsložky, ve kterých mají plné oprávnění uživatelé skupiny test a oprávnění měnit u složky sdílená data pouze jeden nejmenovaný uživatel.

5.2 Sdílení složek v doméně

Aby uživatelé s oprávněným přístupem do těchto složek měli jednodušší přístup, bylo zapotřebí pomocí skupinových politik nastavit automatické mapování složek v doméně. Pro nastavení sdílení jsem zvolil automaticky vytvořenou skupinovou politiku Default Domain Policy, kde v nastavení uživatelů se nachází Preferences a uvnitř Windows settings, ve kterém se již nachází potřebné mapování Drive Maps. Při vytváření nové síťové mapy na složku je možno vybrat ze čtyř akcí a to Create, Replace, Update a Delete. Jelikož jsem potřeboval zavést nové mapování, tak jsem zvolil akci Create. Dále bylo potřeba zadat síťovou cestu ke složce a přidělit jí název a volné diskové písmeno. Volitelnou možností poté je použití pro připojení uživatelské jméno a heslo, ale jelikož je třeba, aby všichni využívali vlastní práva, tuto možnost jsem přeskočil. Poslední položka v základním nastavení je viditelnost, která je základně nastavená jako skrytá, a tak jsem ji také zanechal, neboť ji budou mít zobrazenou pouze uživatelé s přístupem. Aby se upřesnilo mapování pouze pro specifikované uživatele, bylo zapotřebí v záložce Common povolit možnost Item-level Targeting, ve kterém se pomocí výrokové logiky nastaví požadované skupiny a uživatelé. Je zde možno přidat mnoho dalších aspektů, podle kterých se mapování provede například rozsah IP adres, jméno domény, název počítače, časový rozsah nebo rozsah MAC adres. Na následujícím obrázku je vidět konkrétní nastavení pro sdílenou složku Účetnictví.



Obrázek 5.1: *Nastavení specifických uživatelů a skupin*

Pro každou sdílenou složku bylo potřeba tento postup provést zvlášť a aby se vše aplikovalo posledním krokem, bylo potřeba aktualizovat skupinové politiky, to bylo provedeno za pomoci příkazové řádky cmd, kde příkazem „gpudate /force“ se provede aktualizace GPO a sdílené složky tak budou k nalezení v počítači.

Závěr

Odborná praxe ve firmě XEVOS Solutions s.r.o. mi poskytla mnoho nových znalostí a zkušeností do života a poukázala na to, jak probíhá práce ve firmách zaměřených na poskytování systémových služeb a podpory. Při vytváření RADIUS serveru, jsem se musel nejdříve seznámit s využívaným prostředím Hyper-V, přes které se vytvářejí virtuální počítače a systémem Windows server 2016, na kterém jsem danou práci vykonal úspěšně bez větších potíží a nyní se používá ve firemní síti pro připojení na bezdrátovou síť. Důležitým bodem v mé praxi také bylo implementování firemního helpdesku pomocí služby IIS, kde se využívá volně dostupný systém osTicket psaný jazykem PHP. Zde jsem získal mnoho nových znalostí v ohledu práce se systémem pro vyřizování požadavků od klientů. Výsledek této práci je možno nalézt na adrese www.helpdesk.xevos.cz a připravuje se i responzivní zobrazení na mobily a mobilní aplikace. Při další práci na vzdáleném serveru klienta jsem se naučil používat skupinové politiky a jejich implementaci do domény. U posledního bodu jsem narazil na problém se službou SMB, který jsem nakonec vyřešil a podle šablony jsem nastavil přístup uživatelům a namapoval jednotlivé složky do domény.

Použitá literatura

[1] Windows server 2016, http://www.michalzobec.cz/windows-server-2016-novinky-4725, 1.12.2016.

[2] Windows server 2016 licence, https://www.microsoft.com/cs-cz/cloud-platform/windows-server-pricing

[3] Windows server 2016 Essentials, https://en.wikipedia.org/wiki/Windows_Server_Essentials, 17.4.2017

[4] Microsoft Nano Server, http://www.michalzobec.cz/microsoft-nano-server-vse-co-jste-chteli-vedet-3526, 17.8.2015.

[5] Co je Hyper-V, http://svet-hostingu.cz/2009/02/13/co-je-hyper-v/, 13.02.2009

[6] Hyper-V, https://en.wikipedia.org/wiki/Hyper-V, 17.4.2017

[7] Co je to VPN, http://www.vpn-zmenaipadresy.cz/co-je-vpn/

[8] Remote Desktop Protocol, https://en.wikipedia.org/wiki/Remote_Desktop_Protocol

[9] NAS, https://cs.wikipedia.org/wiki/NAS, 21. 12. 2016

[10] Netgear ReadyNAS 104 datasheet, https://www.netgear.com/home/products/connected-storage/RN10400.aspx?cid=wmt_netgear_organic#tab-techspecs

[11] KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě LAN/MAN/WAN a jejich aplikace*. 2., aktualiz. vyd. Praha: Grada Publishing, 2003. ISBN 80-247-0545-1.

[12] RADIUS server, https://cs.wikipedia.org/wiki/RADIUS, 4. 3. 2017